Journal of Universal Computer Science, vol. 3, no. 9 (1997), 1023-1036
submitted: 5/12/96, accepted: 11/7/97, appeared: 28/9/97 *© Springer Pub. Co.*

Linear Multisecret-Sharing Schemes and Error-Correcting Codes

Cunsheng Ding
(Dept of Information Systems & Computer Science
National University of Singapore
Lower Kent Ridge Road, Singapore 119260
dingcs@iscs.nus.edu.sg)

Tero Laihonen
(Department of Mathematics, University of Turku
FIN-20014 Turku, Finland
terolai@sara.utu.fi)

Ari Renvall
(Department of Mathematics, University of Turku
FIN-20014 Turku, Finland
ariren@sara.utu.fi)

Abstract: In this paper a characterization of the general relation between linear multisecret-sharing schemes and error-correcting codes is presented. A bridge between linear multisecret-sharing threshold schemes and maximum distance separable codes is set up. The information hierarchy of linear multisecret-sharing schemes is also established. By making use of the bridge several linear multisecret-sharing threshold schemes based on Reed-Solomon codes, generalized Reed-Solomon codes, Bossen-Yau redundant residue codes are described, which can detect and correct cheatings. The relations between linear multisecret-sharing threshold schemes and some threshold schemes for single-secret sharing are pointed out.

Key Words: Cryptosystems, error-correcting codes, information theory.
Category: E.3

1 Introduction

In a secret-sharing scheme, a dealer has a secret. The dealer gives each participant in the scheme a share of the secret. Let $\mathbf{P}$ denote the set of participants. There is a set $\Gamma \subseteq 2^{\mathbf{P}}$ such that any subset of participants that is in Γ can determine the secret. Since $\mathbf{P}$ is finite, let $\mathbf{P} = \{p_1, ..., p_n\}$. Let $\mathbf{T}_i$ be the set of all possible shares that participant p_i can get, and $\mathbf{T} = \mathbf{T}_1 \times \mathbf{T}_2 \times \cdots \times \mathbf{T}_n$. A scheme is said to be *perfect* if the following properties are satisfied:

1. if a subset B of participants pool their shares, where $B \in \Gamma$, then they can determine the value of s;
2. if a subset B of participants pool their shares, where $B \notin \Gamma$, then they get no information about s.

Since the first construction of secret-sharing schemes by Blakley [1] and Shamir [11], many other schemes have been proposed. Quite a number of them are linear. So far the most studied secret-sharing system is the (m, n) threshold schemes.

A (m, n) threshold scheme is a secret-sharing scheme such that the secret can be constructed from any m shares, but no subset of $m-1$ shares reveals any information about the secret. By definition an (m, n) threshold scheme is perfect.

In [5] Karnin, Greene and Hellman considered the situation where there are k secrets $s_1, s_2, \cdots, s_k$ to be shared, and it is required that for any $1 \leq j \leq k$

C1: any set of m shares determines the secret s_j, i.e., for any set of m indices $1 \leq i_1 < \cdots < i_m \leq n$, $H(s_j|(t_{i_1}, \cdots, t_{i_m})) = 0$, here and hereafter t_i denotes the share of participant p_i;

C2: any set of $m-1$ shares gives no information about the secret s_j, i.e., for any set of $m-1$ indices $1 \leq i_1 < \cdots < i_{m-1} \leq n$, $H(s_j|(t_{i_1}, \cdots, t_{i_{m-1}})) = H(s_j)$, or in terms of mutual information $I(s_j; (t_{i_1}, \cdots, t_{i_{m-1}})) = 0$, where $H(s_j)$ denotes the uncertainty of s_j, $H(a|b)$ the uncertainty of a when event b happened, and $I(a; b)$ denotes the amount of mutual information between a and b.

Such schemes are necessary in applications where a number of secrets should be shared at the same time by a number of participants. We will refer to such systems as $[k, m, n]$ (multisecret-sharing) threshold schemes. Another important fact is that each $[k, m, n]$ threshold scheme for multisecret sharing gives naturally k (m, n) threshold schemes for single-secret sharing. Thus, the importance of multisecret sharing follows also from that of single-secret sharing.

A threshold scheme for multisecret sharing was proposed by Karnin, Green and Hellman in [5]. Multisecret sharing schemes were also studied by Jackson, Martin, and O'Keefe [4], where they considered the case in which each subset of k participants is associated with a secret which is protected by a (t, k)-threshold access structure and lower bounds on the size of a participant's share. Some information aspects of multisecret sharing schemes were also studied by Blundo, De Santis, Di Crescenzo Gaggia, and Vaccaro [2], where they tried to work out a general theory of multisecret sharing schemes and to establish some lower bounds on the size of information held by each participant for various access structures.

In this paper we first consider the general relation between linear multisecret-sharing schemes and error-correcting codes in Section 2. In Section 3 we establish the relation between linear $[k, k, n]$ threshold schemes for multisecret sharing and maximum distance separable (MDS) linear codes. Then in Section 4 we construct some $[k, k, n]$ threshold schemes for multisecret sharing based on some redundant residue MDS codes. Finally, we show how to use a multisecret-sharing scheme as a threshold scheme for single secret-sharing, and some relations between single-secret sharing and multisecret sharing.

The contributions of this paper are the following:

1. a characterization of the general relation between linear multisecret sharing schemes and error-correcting codes;
2. a bridge between linear multisecret-sharing threshold schemes and maximum distance separable codes;
3. the establishment of the information hierarchy of linear multisecret sharing schemes;
4. several linear multisecret sharing threshold schemes that are based on Reed-Solomon codes, generalized Reed-Solomon codes, and Bossen-Yau redundant residue codes, which can detect and correct cheatings;

5. the relations between linear multisecret sharing threshold schemes and some threshold schemes for single-secret sharing.

2 The General Relation

It is reasonable to assume that each element of the secret space $\mathbf{S}_i$ is equally likely to be the ith secret for each i. Let the secret spaces $\mathbf{S}_i$ for each $1 \leq i \leq k$ and the share spaces $\mathbf{T}_i$ for each $1 \leq i \leq n$ be vector spaces over a field F. Then the product spaces $\mathbf{S} = \mathbf{S}_1 \times \cdots \times \mathbf{S}_k$ and $\mathbf{T} = \mathbf{T}_1 \times \cdots \times \mathbf{T}_n$ are also vector spaces over F. In a multisecret-sharing scheme a dealer uses a *share function* $f : \mathbf{S} \to \mathbf{T}$ to compute the shares for the n participants, i.e., let $\mathbf{s} = (s_1, \cdots, s_k)$ be the vector consisting of k secrets s_i and $\mathbf{t} = (t_1, \cdots, t_n) = f(\mathbf{s})$, the share given only to the ith participant is t_i. Clearly, the share function must be one-to-one. A multisecret-sharing scheme is said to be *linear* if for all $a, a' \in F$ and all $s, s' \in \mathbf{S}$

$$f(as + a's') = af(s) + a'f(s'). \tag{1}$$

If there is a constant $t \in \mathbf{T}$ such that $f(x) - t$ is linear, then the secret-sharing scheme is said to be *affine*.

In what follows we consider the case that $\mathbf{S}_i = F$ and $\mathbf{T}_i = F$, where $F = GF(q)$ is a field. Thus, $\mathbf{T} = F^n$ and $\mathbf{S} = F^k$ both are vector spaces over F. We restrict ourselves to the case F being finite since in many applications only the finite case is interesting.

Theorem 1. *A multisecret-sharing scheme defined over the above secret and share spaces is linear if and only if its share function is of the form*

$$f(\mathbf{s}) = \mathbf{s}G, \tag{2}$$

where $\mathbf{s} = (s_1, \cdots, s_k) \in \mathbf{S}$*, and* G *is a* $k \times n$ *matrix over* F *with rank* k*.*

Proof: Let $\mathbf{e}_i \in F^k$ be the vector with the ith entry being the identity element 1 and other entries being the zero element of F. Note that every vector $\mathbf{s} \in F^k$ can be expressed as $\mathbf{s} = \sum_{i=1}^{k} s_i \mathbf{e}_i$, where $s_i \in F$. Assume that the scheme is linear, then

$$f(\mathbf{s}) = f\left(\sum_{i=1}^{k} s_i \mathbf{e}_i\right) = \sum_{i=1}^{k} s_i f(\mathbf{e}_i) = \mathbf{s}G,$$

where G is the matrix with $f(\mathbf{e}_i)$ as its ith row. Since each $\mathbf{t} = (t_1, \cdots, t_n) \in F^n$ corresponds to at most one preimage under the mapping f, the rank of the matrix G must be k.

If the share function of a secret-sharing scheme is of form (2) where G has rank k, then it is easily seen that the scheme is linear. $\square$

An $[n, k, d]$ linear code $\mathcal{C}$ over F is a linear subspace of F^n with dimension k and minimum distance d, where the distance of two codewords $\mathbf{u}$ and $\mathbf{v} \in F^n$ is the number of different entries. A $k \times n$ matrix G over F is called a *generator* matrix of $\mathcal{C}$ if its row vectors generate the linear subspace $\mathcal{C}$, i.e., $\mathcal{C} = \{\mathbf{c} = \mathbf{i}G : \mathbf{i} \in F^k\}$. For a linear code $\mathcal{C}$ its dual code, denoted as $\mathcal{C}^\perp$, is defined by

$$\mathcal{C}^\perp = \{\mathbf{u} \in F^n : \mathbf{u}\mathbf{v}^T = 0 \text{ for all } \mathbf{v} \in \mathcal{C}\}.$$

A generator matrix H of $\mathcal{C}^\perp$ is called the parity check matrix of $\mathcal{C}$. Thus, $GH^T = 0_{k\times(n-k)}$.

Theorem 1 clearly shows that a linear multisecret-sharing scheme gives an $[n, k, d]$ (linear) code $\mathcal{C}$ with generator matrix G, and each generator matrix G of an $[n, k, d]$ linear code $\mathcal{C}$ gives a linear multisecret-sharing scheme. The share function is an encoding mapping of a linear code.

For a linear multisecret-sharing scheme with the share function f of (2), recovering the original multisecret $\mathbf{s}$ is carried out as follows. Let $G(i_1, \cdots, i_u)$ denote the submatrix consisting of the i_1th, i_2th, ..., i_uth columns of the matrix G, where $1 \le u \le n$, and $1 \le i_1 < \cdots < i_u \le n$. Suppose that the shares t_{i_1}, ..., t_{i_u} are known, then recovering the multisecret becomes solving the linear equation

$$\mathbf{s}G(i_1, \cdots, i_u) = (t_{i_1}, \cdots, t_{i_u}). \tag{3}$$

The complexity of solving such a linear equation is $O(u^3)$ with a method like the Gaussian elimination method. Thus, recovering the multisecret is much simpler than decoding linear codes.

3 Linear $[l, m, n]$ Threshold Schemes and MDS Codes

Since we have assumed that the secrets from each secret space $\mathbf{S}_i$ are equally likely, without the knowledge of any share the uncertainty (denoted as $H(s_i)$) or self-information (denoted as $I(s_i)$) of each s_i is $H(s_i) = I(s_i) = \log_2 q$ bits, and the uncertainty or self-information of each $\mathbf{s} = (s_1, \cdots, s_k)$ is $I(\mathbf{s}) = H(\mathbf{s}) = k \log_2 q$ bits, here we assume that all secrets are independent. To recover the multisecret, a set of shares must provide $I(\mathbf{s})$ bits of information about the secret.

Theorem 2. *Let a multisecret-sharing scheme have the share function of (2). Then*

$$I(\mathbf{s}; (t_{i_1}, \cdots, t_{i_u})) = r \log_2 q = \begin{cases} < I(\mathbf{s}), & \textit{iff } r < k; \\ = I(\mathbf{s}), & \textit{iff } r = k; \end{cases}$$

$$H(\mathbf{s}|(t_{i_1}, \cdots, t_{i_u})) = (k-r) \log_2 q = \begin{cases} > 0, & \textit{iff } r < k; \\ = 0, & \textit{iff } r = k; \end{cases}$$

where $r = \mathrm{rank} G(i_1, \cdots, i_u)$.

Proof: Since the rank of the matrix $G(i_1, \cdots, i_u)$ is r, by elementary algebra Equation (3) has q^{k-r} solutions and each of them is equally likely to be the multisecret. It follows that $H(\mathbf{s}|(t_{i_1}, \cdots, t_{i_u})) = (k-r) \log_2 q$ bits, and that

$$I(\mathbf{s}; (t_{i_1}, \cdots, t_{i_u})) = I(\mathbf{s}) - H(\mathbf{s}|(t_{i_1}, \cdots, t_{i_u})) = r \log_2 q.$$

The remaining conclusions then follow easily. □

By Theorem 2 the amount of information about the multisecret $\mathbf{s}$ given by a set of shares $\{t_{i_1}, \cdots, t_{i_u}\}$ is completely determined by the rank of the submatrix $G(i_1, \cdots, i_u)$ of G. Thus, each share gives information about the multisecret $\mathbf{s}$, however we shall prove this could not be true for each individual secret s_j.

Theorem 3. *Let a multisecret-sharing scheme have the share function of Equation (2). If* $r = \text{rank}G(i_1, \cdots, i_u) = k$ *then*

$$I(s_j; (t_{i_1}, \cdots, t_{i_u})) = \log_2 q = I(s_j);$$
$$H(s_j|(t_{i_1}, \cdots, t_{i_u})) = 0.$$

If $r < k$ *then* $I(s_j; (t_{i_1}, \cdots, t_{i_u})) = \log_2 q = I(s_j)$ *if and only if the vector* $\mathbf{e}_j$ *is a linear combination of the column vectors of the submatrix* $G(i_1, \cdots, i_u)$*; otherwise* $I(s_j; (t_{i_1}, \cdots, t_{i_u})) = 0$.

Proof: By elementary algebra Equation (3) has q^{k-r} solutions and each of them is equally likely to be the multisecret. If $r = k$, the multisecret is determined by the set of shares, and so is each individual secret s_j.

If $r < k$, then Equation (3) has $q^{k-r} \geq q$ solutions. Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ denote the column vectors of G. Assume first that $\mathbf{e}_j$ is a linear combination of the column vectors of $G(i_1, \cdots, i_u)$, i.e., there are constants $a_{i_1}, \cdots, a_{i_u}$ such that

$$\mathbf{e}_j = \sum_{v=1}^{u} a_{i_v} \alpha_{i_v}.$$

It follows that

$$s_j = \mathbf{s}\mathbf{e}_j = \sum_{v=1}^{u} a_{i_v} \mathbf{s} \alpha_{i_v}$$
$$= \sum_{v=1}^{u} a_{i_v} t_{i_v}.$$

Thus, s_j can be recovered by the shares $t_{i_1}, \cdots, t_{i_u}$.

Assume that $\mathbf{e}_j$ cannot be expressed as a linear combination of $\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_u}$. Note that the rank of G is k, there must be $j_1, \cdots, j_v \notin \{i_1, \cdots, i_u\}$ such that $\mathbf{e}_j$ is a linear combination of

$$\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_u}, \alpha_{j_1}, \cdots, \alpha_{j_v},$$

where $u + v \leq n$. Let

$$\mathbf{e}_j = \sum_{w=1}^{u} a_w \alpha_{i_w} + \sum_{w=1}^{v} b_w \alpha_{j_w}.$$

By assumption at least one of the coefficients b_w is nonzero, say, $b_1 \neq 0$. It follows that

$$s_j = \mathbf{s}\mathbf{e}_j = \sum_{w=1}^{u} a_w \mathbf{s} \alpha_{i_w} + \sum_{w=1}^{v} b_w \mathbf{s} \alpha_{j_w}$$
$$= \sum_{w=1}^{u} a_w t_{i_w} + \sum_{w=1}^{v} b_w t_{j_w}.$$

Since t_{j_1} is unknown and equally likely to be any element of $GF(q)$, the set of shares $\{t_{i_1}, \cdots, t_{i_u}\}$ gives no information about s_j. □

In the sequel we study only $[k, k, n]$ linear multisecret-sharing schemes. Linear $[n, k, d]$ codes with $d = n - k + 1$ are called MDS (maximum distance separable).

Theorem 4. *A multisecret-sharing scheme with the share function of (2) is a* $[k, k, n]$ *threshold scheme if and only if*

D1: the linear code $\mathcal{C}$ *with generator matrix* G *is MDS; and*
D2: any set of $k-1$ *column vectors of* G *generates a* $[k, k-1, 2]$ *MDS code.*

Proof: Recall that for an $[n, k, d]$ linear code $\mathcal{C}$ over $GF(q)$ the following statements are equivalent [6]:

S1: $\mathcal{C}$ is MDS;
S2: every k columns of a generator matrix G are linearly independent;
S3: every $n - k$ columns of a parity check matrix H are linearly independent.

Assume that Conditions D1 and D2 are satisfied. By Statement S2 every k columns of G are linearly independent. Thus, every set of k shares is sufficient to determine the multisecret $\mathbf{s}$ by Theorem 3. Obviously, the rank of every $k-1$ columns of G is less than k. In addition, Condition D2 ensures that each vector $\mathbf{e}_i$ is not a linear combination of any $k-1$ column vectors of G. Thus, by Theorem 3 it is a $[k, k, n]$ linear multisecret-sharing scheme.

Assume that the multisecret sharing system is a $[k, k, n]$ threshold scheme. Note that the rank of any set of $k-1$ vectors is less than k, by Theorem 3 each $\mathbf{e}_i$ cannot be generated by any set of $k-1$ column vectors of G. Thus, any $k-1$ column vectors of G generate a linear code with minimum distance ≥ 2. We now prove that any k column vectors of G have rank k. Without loss of generality we consider the first k columns of G, denoted by $\mathbf{g}_1, \cdots, \mathbf{g}_k$. Suppose now that

$$\mathrm{rank}(\mathbf{g}_1, \mathbf{g}_2, \cdots, \mathbf{g}_k) < k.$$

Since the first k shares determine the secret, by Theorem 3 each $\mathbf{e}_i$ is a linear combination of $\mathbf{g}_1, \cdots, \mathbf{g}_k$. Thus, each $\mathbf{e}_i$ is a linear combination of $k-1$ vectors of those $\mathbf{g}_1, \cdots, \mathbf{g}_k$. It follows again by Theorem 3 that some $k-1$ shares can determine the multisecret. This is contrary to the definition of a $[k, k, n]$ threshold scheme. Hence, any k column vectors of G are linearly independent. By Statement S2 the linear code generated by G is MDS.

Note that any k column vectors of G are linearly independent, any set of $k-1$ column vectors of G has rank $k-1$, and thus generates a $[k, k-1, d]$ code. By the Singleton bound in coding theory $d \leq k - (k-1) + 1 = 2$. Combining this with the above proved fact $d \geq 2$ gives $d = 2$. □

By Theorem 4 one $[k, k, n]$ threshold scheme for multisecret sharing gives one $[n, k, n-k+1]$ MDS code and k MDS codes with parameters $[k, k-1, 2]$.

Theorem 5. *For any linear* $[k, k, n]$ *threshold scheme with the share function of (2)*

$$I(\mathbf{s}; (t_{i_1}, \cdots, t_{i_u})) = \min\{k, u\} \log_2 q.$$

Proof: Consider the matrix $G(i_1, \cdots, i_u)$. If $u \geq k$, then $I(\mathbf{s}; (t_{i_1}, \cdots, t_{i_u})) = k \log_2 q$, as desired. If $u < k$, without loss of generality, let $i_j = j$ for $j = 1, ..., u$. It follows that $u \geq \text{rank}G(1, ..., u) \geq \text{rank}G(1, ..., k) - (k - u) = u$ and that $\text{rank}G(i_1, \cdots, i_u) = u$. The conclusion then follows from Theorem 2. □

This theorem clearly shows the information hierarchy about the multisecret of $[k, k, n]$ threshold schemes, i.e., $I(\mathbf{s}; B) = |B| \log_2 q$, where B is a set of shares. Thus, linear $[k, k, n]$ threshold schemes are the most democratic schemes in that each share contains the same amount of information about the multisecret, and two sets of shares give the same amount of information about the multisecret if and only if the numbers of shares in the two sets are equal. However, the information hierarchy about each individual secret s_j is quite different, i.e., $I(s_j; B) = 0$ if $|B| < k$ and $I(s_j; B) = I(s_j)$ otherwise.

The relation between linear $[k, k, m]$ threshold schemes and linear $[n, k, n - k + 1]$ MDS codes is now clear. To construct such multisecret-sharing schemes, we need to find linear MDS codes. It is obvious that not every generator matrix of an MDS code satisfies condition D2. So our task is first to find MDS codes, and then to find generator matrices of those codes satisfying condition D2. In some of the following sections we shall consider linear $[k, k, n]$ threshold schemes based on the following MDS codes: Reed-Solomon (or RS) codes, extended RS codes, generalized RS codes, and Bossen-Yau codes, which are MDS codes. Finding more linear $[k, k, n]$ threshold schemes means finding more MDS codes. This is related to othorgonal arrays and also othorgonal Latin squares. For some of the relations we refer to [6, pp. 328-329].

4 $[k, k, n]$ Threshold Schemes via Redundant Residue Codes

RS codes are special redundant residue codes which include other MDS codes. Let $m_0(x)$, $\cdots$, $m_{s+t-1}(x) \in GF(q)[x]$ be pairwise relatively prime, with degree m, s and t be two positive integers, and $k = sm$. For each polynomial $p(x)$ of degree no more than $k - 1$, define

$$\begin{aligned} r_i(x) &= p(x) \bmod m_i(x),\ i = 0, 1, \cdots, s + t - 1 \\ &= r_{i,0} + r_{i,1}x + \cdots + r_{i,m-1}x^{m-1} \end{aligned}$$

and $\mathbf{r}_i = (r_{i,0}, \cdots, r_{i,m-1})$. A special redundant residue code investigated by Bossen and Yau [3] is described by

$$\mathcal{C} = \{(\mathbf{r}_0, \mathbf{r}_1, \cdots, \mathbf{r}_{s+t-1}) | p(x) \in GF(q)[x]_k\}.$$

This is an $[(s + t)m, sm, d]$ linear code. Under one basis of $GF(q^m)$ over $GF(q)$ each $\mathbf{r}_i$ is viewed as an element of $GF(q^m)$, and the code is transferred into an $[s + t, s, t + 1]$ MDS code $\mathcal{C}'$ over $GF(q^m)$.

Redundant residue codes and their generalized codes encompass a number of good codes including the Reed-Solomon codes. Some of them can be used to construct linear $[k, k, n]$ threshold schemes. In this section we shall describe some linear $[k, k, n]$ threshold schemes based on redundant residue MDS codes.

A class of MDS codes is the RS codes [6, pp.303-304]. Let $\alpha = (\alpha_1, \cdots, \alpha_n)$ where the α_i are distinct elements of $GF(q)$. The $[n, k, n - k + 1]$ RS code is generated by the following generator matrix

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}. \tag{4}$$

To construct linear multisecret-sharing $[k, k, n]$ threshold schemes based on the RS code, we need the following lemma.

Lemma 6. *Any $(k-1) \times (k-1)$ submatrix of the G of (4) has rank $k-1$ if and only if for any set of indices $1 \le i_1 < \cdots < i_{k-1} \le n$*

$$\sum_{1 \le u_1 < \cdots < u_j \le k-1} \alpha_{i_{u_1}} \alpha_{i_{u_2}} \cdots \alpha_{i_{u_j}} \ne 0 \textit{ for all } j = 1, 2, \cdots, k-2. \tag{5}$$

Proof: Let $a_1, \cdots, a_{k-1}$ be $k-1$ distinct elements over $GF(q)$. Define

$$M = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_{k-1} \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{k-1} & a_2^{k-1} & \cdots & a_{k-1}^{k-1} \end{bmatrix}_{k \times (k-1)}.$$

Let M_i denote the matrix obtained by deleting the ith row of M, where $1 \le i \le k$.

Consider now the following determinant

$$V = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ x & a_1 & a_2 & \cdots & a_{k-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x^{k-1} & a_1^{k-1} & a_2^{k-1} & \cdots & a_{k-1}^{k-1} \end{vmatrix}.$$

Expanding this determinant according to the first column, we obtain that

$$V = |M_1| - |M_2|x + \cdots + (-1)^{k+1}|M_k|x^{k-1}, \tag{6}$$

where $|M_i|$ denotes the determinant of M_i for each i.

On the other hand, V is the determinant of a Vandermonde matrix and thus

$$V = (a_1 - x)(a_2 - x) \cdots (a_{k-1} - x)a \tag{7}$$

$$= a \sum_{j=0}^{k-1} \left(\sum_{1 \le u_1 < \cdots < u_{k-1-j} \le k-1} a_{u_1} a_{u_2} \cdots a_{u_{k-1-j}} \right) (-1)^j x^j, \tag{8}$$

where

$$a = \prod_{j=1}^{k-2} \prod_{i=j+1}^{k-1} (a_i - a_j).$$

Comparing the coefficients of (6) and (7), we get the determinant M_i for each i. The conclusion of this lemma then follows. □

The linear multisecret-sharing scheme based on RS codes is constructed as follows. Choose the α_i such that (5) holds. Then we use the matrix of Equation (4) as the one of (2) to construct the share function for the multisecret-sharing scheme.

Theorem 7. *The multisecret-sharing scheme based on the RS code with generator matrix G of (4) satisfying (5) is a linear $[k, k, n]$ threshold scheme.*

Proof: Clearly, the RS code is MDS since every k columns of G are linearly independent. What remains to be shown is that any $k-1$ column vectors of G generate a linear code with minimum distance ≥ 2. Consider now the i_1th, i_2th, $\cdots$, i_{k-1}th columns $\mathbf{g}_{i_1}$, $\mathbf{g}_{i_2}$, $\cdots$, $\mathbf{g}_{i_{k-1}}$ of G. We now prove that each vector $\mathbf{e}_j$ cannot be a linear combination of the vectors $\mathbf{g}_{i_s}$, where $1 \leq j \leq k$.

Suppose that $\mathbf{e}_j = \sum_{s=1}^{k-1} x_s \mathbf{g}_{i_s}$. Then we have the following equations

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{i_1}^{j-1} & \alpha_{i_2}^{j-1} & \cdots & \alpha_{i_{k-1}}^{j-1} \\ \alpha_{i_1}^{j+1} & \alpha_{i_2}^{j+1} & \cdots & \alpha_{i_{k-1}}^{j+1} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{i_1}^{k-1} & \alpha_{i_2}^{k-1} & \cdots & \alpha_{i_{k-1}}^{k-1} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ \vdots \\ \vdots \\ x_{k-1} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{bmatrix} \tag{9}$$

and

$$\sum_{s=1}^{k-1} x_s \alpha_{i_s}^j = 1. \tag{10}$$

Since the elements α_i satisfy (5), the coefficient matrix of (9) is invertible by Lemma 6. It follows that $x_i = 0$ for each i. But this makes the lefthand of Equation (10) equal zero, a contradiction. Thus, each vector $\mathbf{e}_j$ cannot be a linear combination of $k-1$ column vectors of G. Hence Condition D2 is satisfied. By Theorem 4 it is a $[k, k, n]$ threshold scheme. □

To illustrate the above linear multisecret-sharing $[k, k, n]$ threshold scheme based on RS codes, we take the following example.

Example 1 Consider the field $GF(11) = Z/(11)$ and $k = 3$. Let $\alpha_i = i$ for $i = 1, 2, 3, 4, 5$. Then the matrix in (4) becomes

$$G' = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 9 & 5 & 3 \end{bmatrix},$$

which generates a $[5, 3, 3]$ MDS code over $GF(11)$. It is easily checked that each 2×2 submatrix of G' is invertible, so G' gives a $[3, 3, 5]$ threshold scheme for multisecret sharing. □

By adding a parity check symbol, each $[n, k, n-k+1]$ RS code can be extended into an $[n+1, k, n-k+2]$ MDS code if $n < q$. Such an MDS code could also be used to construct multisecret-sharing $[k, k, n+1]$ threshold schemes by choosing proper elements for the matrix G.

A more general class of MDS codes is the generalized RS codes. Let $\alpha = (\alpha_1, \cdots, \alpha_n)$ where the α_i are distinct elements of $GF(q)$, and $\mathbf{v} = (v_1, \cdots, v_n)$ where the v_i are nonzero (but not necessarily distinct) elements of $GF(q)$. The generalized RS code, denoted by $GRS_k(\alpha, \mathbf{v})$, is generated by the following matrix

$$G = \begin{bmatrix} v_1\alpha_1^0 & v_2\alpha_2^0 & \cdots & v_n\alpha_n^0 \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ \vdots & \vdots & \vdots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \cdots & v_n\alpha_n^{k-1} \end{bmatrix}. \tag{11}$$

This is an $[n, k, n-k+1]$ MDS code. When $v_1 = v_2 = \cdots = v_n = 1$ it is the Reed-Solomon code. Linear multisecret-sharing $[k, k, n]$ threshold schemes based on the generalized RS codes can be similarly constructed as described in the following theorem.

Theorem 8. *Choose n elements $\alpha_i \in GF(q)$ such that (5) holds for each $1 \leq j \leq k-2$. Then the linear multisecret-sharing scheme of (2) with the matrix G of (11) is a $[k, k, n]$ threshold scheme.*

The proof of this theorem is similar to that of Theorem 7.

Example 2 As an example of the linear multisecret-sharing schemes based on generalized RS codes, we consider again the field $GF(11)$ and $k = 3$. Let $\alpha_i = i$ for $i = 1, 2, 3, 4, 5$ and $v_1 = 1$, $v_2 = 2$, $v_3 = 3$, $v_4 = 5$ and $v_5 = 6$. The matrix of (11) then becomes

$$G'' = \begin{bmatrix} 1 & 2 & 3 & 5 & 6 \\ 1 & 4 & 9 & 9 & 8 \\ 1 & 8 & 5 & 3 & 7 \end{bmatrix},$$

which generates a $[5, 3, 3]$ generalized RS code. Since each 2×2 submatrix of G'' is invertible, G'' gives a multisecret-sharing $[3, 3, 5]$ threshold scheme. □

With the Bossen-Yau code $\mathcal{C}'$ defined at the begining of this section, a linear multisecret-sharing scheme could be similarly constructed by choosing the moduli properly. This code can also be generalized in the same way for RS codes, and linear multisecret-sharing threshold schemes based on them could be similarly constructed. We shall not go into these multisecret-sharing schemes in detail.

5 From $[k, k, n]$ to (k, n) Threshold Schemes

Multisecret-sharing $[k, m, n]$ threshold schemes are designed for sharing a set of k independent secrets among n participants. Naturally, it can be used as an (m, n) threshold scheme for sharing one secret among n participants as follows. For simplicity, we assume that $\mathbf{S}_i$ are the same. Let s_i be the single secret to be shared among n participants, choose randomly $k-1$ values for $s_1, \cdots, s_{i-1}, s_{i+1}, \cdots, s_k$. Then compute and distribute the shares to the n participants as the same as for multisecret sharing. When m shares are available, compute the vector $\mathbf{s} = (s_1, \cdots, s_k)$ and thus obtain the required secret s_i. By the definition of multisecret-sharing systems this gives an (m, n) threshold scheme for single secret sharing.

It is important to note when a multisecret-sharing $[k, m, n]$ threshold system is used for single secret-sharing, the single secret can be put as any coordinate of $\mathbf{s}$. A multisecret-sharing $[k, k, n]$ threshold scheme gives k distinct (k, n) threshold schemes for single-secret sharing. It should be noted that (k, n) threshold schemes for single secret-sharing may not be simply used as $[k, k, n]$ threshold schemes for multisecret-sharing. To demonstrate this, we take the Shamir scheme as an example.

Example 3 Shamir's scheme starts with a polynomial

$$s(x) = s_0 + s_1 x + \cdots + s_{k-1} x^{k-1} \in GF(q)$$

and nonzero distinct elements α_i for $i = 1, 2, \cdots, n$. The single secret to be shared is s_0. The shares are computed as $t_i = s(\alpha_i)$. This is a (k, n) threshold scheme for single secret sharing. One may think this can be used directly as a $[k, k, n]$ threshold scheme by taking $s_1, \cdots, s_{k-1}$ as $k-1$ other secrets. This could be wrong. For example, take $q = 5$, and $\alpha_i = i$ for $i = 1, 2, 3, 4$. If the Shamir $(3, 4)$ threshold scheme is used for sharing three secrets s_0, s_1, s_2 among four participants, it is not a $[3, 3, 4]$ threshold scheme for multisecret sharing, since knowing two shares t_1 and t_4 determines the second secret s_1 although they give no information about each of the other two secrets s_0 and s_2. It should also be noted that in the Shamir's scheme for single-secret sharing, the secret can also be hidden in the last coefficient s_{k-1}, but may not be hidden in $s_1, s_2, \cdots, s_{k-2}$, depending on the choice of the α_i's. $\square$

Clearly, the requirements for multisecret sharing are much stronger than those for single secret sharing. That is why a $[k, m, n]$ threshold scheme can be easily used as an (m, n) threshold scheme for single secret sharing, but the converse is not true for many (m, n) threshold schemes for single secret sharing.

It is not hard to see that not every MDS code can be used to construct linear multisecret-sharing threshold schemes since it is possible that an MDS code has no generator matrix satisfying condition D2. However, it is possible to use such an MDS code for single-secret sharing.

Theorem 9. *An $[n, k, n-k+1]$ MDS code $\mathcal{C}$ over $GF(q)$ can be used to construct a (k, n) threshold scheme for single-secret sharing if it has a generator matrix G such that one of the vectors $\mathbf{e}_i$ cannot be a linear combination of any $k-1$ column vectors of G.*

Proof: Without loss of generality, assume that $\mathbf{e}_1$ is not a linear combination of any $k-1$ column vectors of a generator matrix G. Then the (k, n) threshold scheme based on the MDS code is described as follows. Let s_1 be the single secret to be shared among n participants. Choose randomly $s_2, \cdots, s_k \in GF(q)$. Let $\mathbf{s} = (s_1, \cdots, s_k)$. The n shares t_i are taken as $\mathbf{t} = (t_1, \cdots, t_n) = \mathbf{s}G$. By the definition of $[k, k, n]$ threshold schemes and the proof of Theorem 4 this is a (k, n) threshold scheme for single-secret sharing. $\square$

Clearly, given a generator matrix G of an $[n, k, n-k+1]$ MDS code, if each of $\mathbf{e}_{i_1}, \cdots, \mathbf{e}_{i_h}$ is not a linear combination of any $k-1$ column vectors of G, then the single secret can be put into any of the i_jth coordinate.

6 Against Cheating

In schemes for single-secret sharing some participants may present a falsified share for cheating. For multisecret-sharing this problem is the same as for single-secret sharing. By the connection between linear multisecret-sharing schemes and linear codes established by Theorems 1 and 4, linear multisecret-sharing schemes have the ability to detect cheating and to correct cheating provided that the corresponding linear codes have the ability to detect and correct errors. This can be done directly by error-detecting and error-correcting techniques in coding theory.

The $[k, k, n]$ threshold schemes for multisecret-sharing schemes based on MDS codes are attractive in against cheating since there are efficient decoding algorithms for those codes. Assume that $k + j$ participants have presented their shares for recovering the secret.

Theorem 10. *A $[k, k, n]$ threshold scheme for multisecret sharing can correct up to $\lfloor (n-k)/2 \rfloor + k + j - n$ cheaters when $k + j$ participants come together for the secret.*

Proof: Let G be its matrix in (2). Then G is the generator matrix of an $[n, k, n-k+1]$ MDS code. So it can correct $\lfloor (n-k)/2 \rfloor$ errors. Suppose among the $k + j$ participants there are t cheaters. If $t \leq \lfloor (n-k)/2 \rfloor + k + j - n$, choose randomly $n - k - j$ values for the other $n - j - k$ shares held by the other $n - j - k$ participants. Then there are at most $\lfloor (n-k)/2 \rfloor$ errors in the n shares. Thus, the t errors can be corrected. □

It is easily seen that to have the ability to correct cheaters, the parameter j should satisfy $(n - k + 2)/2 \leq j \leq n - k$. When all n participants come together, the system can correct $\lfloor (n-k)/2 \rfloor$ cheaters and detect $n - k$ cheaters. This is practically feasible since there are efficient decoding algorithms for some MDS codes.

7 Concluding Remarks

Some relations between linear threshold schemes for single-secret sharing and some MDS codes were noticed by McEliece and Sarwate [9] and by Karnin, Green and Hellman [5]. McEliece and Sarwate pointed out the relation between Shamir's scheme and Reed-Solomon codes and gave some generalization where each RS code is applicable for single-secret sharing, while we have used RS codes and generalized RS codes for multisecret-sharing where only RS codes with a generator matrix satisfying condition D2 are applicable. This shows the difference. It is easy to give examples to show that not every MDS code has a generator matrix satisfying condition D2.

Karnin, Green and Hellman [5] suggested a method for single-secret sharing which is equivalent to using MDS codes for single-secret sharing. They also suggested a method based on matrices for multi-secret sharing [5], but it is not known whether their approach to multi-secret sharing can be formulated into one based on codes. In this paper we have used special MDS codes for multi-secret sharing, and only special MDS codes can be used within our approach, as shown clearly by Theorems 4 and 9. The approach we considered in this paper can be viewed as an extension of McEliece and Sarwate's generalization of the Shamir scheme. However, our main concern here is multisecret-sharing while Shamir, McEliece and Sarwate considered only single-secret sharing. We refer to the approach considered in the paper as the coding approach since

1. in single-secret sharing the secret is a component of the information vector and the shares form *all* components of the codeword corresponding to the information vector;
2. in multisecret sharing the multisecret is *exactly* the information vector and shares form the *exact* codeword corresponding to the information vector.

The advantage of the coding approach is that cheating correction and detection are convenient since each share vector is a codeword of the codes generated by the matrix G, but the disadvantage is that special MDS codes are needed.

Some applications of codes in secret-sharing were considered by Massey [7, 8], where the concept of minimal codewords was introduced to characterize the access structure of some single-secret sharing schemes based on codes.

Since this paper is only about linear multisecret sharing based on codes, we could not mention the vast achievement in single-secret sharing here. However, we have mentioned all relevant results to this topic which we are aware of. For some information about single secret sharing, we refer to [10, 12, 13, 14, 15].

References

1. G. R. Blakley, *Safeguarding cryptographic keys,* Proc. NCC AFIPS 1979, 313–317.
2. C. Blundo, A. De Santis, G. Di Cresceno, A. Gaggia, and U. Vaccaro, *Multi-secret sharing schemes,* Advances in Cryptology: Crypto'93, LNCS 773, Springer-Verlag, 1993, 126–135.
3. D. C. Bossen and S. S. Yau, *Redundant residue polynomial codes,* Information and Control, 13 (1968), 597–618.
4. W. A. Jackson, K. M. Martin, and C. M. O'Keefe, *Multisecret threshold schemes,* Advances in Cryptology: Crypto'94, LNCS 839, Springer-Verlag, 1994, 150–163.
5. E. D. Karnin, J. W. Green and M. Hellman, *On secret sharing systems,* IEEE Trans Inform. Theory, Vol. IT-29 (1983), 35–41.
6. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, 1978.
7. J. L. Massey, *Minimal codewords and secret sharing,* Proc. 6th Joint Swedish-Russian Workshop on Inform. Theory, Mölle, Sweden, August 22–27, 1993, 276–279.
8. J. L. Massey, *Some applications of coding theory in cryptography, in* Codes and Cyphers: Cryptography and Coding IV (Ed. P. G. Farrell). Esses, England: Formara Ltd., 1995, 33–47.
9. R. J. McEliece and D. V. Sarwate, *On sharing secrets and Reed-Solomon codes,* Comm. ACM, Vol. 24 (1981), 583–584.
10. A. Salomaa, *Public-Key Cryptography,* Heidelberg: Springer, 1990, 187–190.
11. A. Shamir, *How to share a secret,* Comm. ACM, Vol. 22, 1979, 612-613.
12. G. J. Simmons, *How to (really) share a secret,* Proc. Crypto'88, LNCS 403, Springer 1989, 390–448.
13. G. J. Simmons, *Geometric shared secret and/or shared control schemes,* Proc. Crypto'90, LNCS 537, Springer 1991, 216–241.
14. D. R. Stinson and S. A. Vanstone, *A combinatorial approach to threshold schemes,* SIAM J. Disc. Math, vol. 1, No. 2 (1988), 230–236.

15. Y. Zheng, T. Hardjono, and J. Seberry, *Reusing shares in secret sharing schemes*, The Computer Journal 37 (1994), 199–205.